UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MICHIGAN

JONI LIPSON, on behalf of herself and all others similarly situated, Plaintiff, v. WELLTOK LLC. and COREWELL HEALTH EAST, Defendant.	Case No. **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff, Joni Lipson, on behalf of herself and all others similarly situated, states as follows for her class action complaint against Defendants Welltok LLC, ("Welltok") and Corewell Health East ("Corewell") (collectively "Defendants"):

INTRODUCTION

1. On May 30, 2023, Welltok, an enterprise SaaS company that partners with healthcare companies, lost control over its computer network and the highly private information stored on the computer network in a data breach perpetrated by cybercriminals ("Data Breach"). On information and belief, the Data Breach's impact has been substantial, affecting thousands of its clients' patients.

2. Corewell, a healthcare company based in Michigan, chose to allow Welltok access and control over its patients' highly sensitive personal and health information.

3. Welltok's breach differs from typical data breaches because it affects patients who had no relationship with Welltok, never sought one, and never consented to Welltok collecting and

storing their information.

4. On information and belief Data Breach began on or around May 30, 2023, but was not discovered by Defendants until July 26, 2023. Following an internal investigation, Defendants learned cybercriminals gained unauthorized access to Corewell's former and current patients' personally identifiable information ("PII") and private health information ("PHI") (collectively with PII, "Sensitive Information").

5. On information and belief, cybercriminals bypassed Welltok's inadequate security systems to access Corewell's patients' Sensitive Information in its computer systems.

6. On or about November 17, 2023, Defendants finally notified State Attorneys General and many Class Members about the widespread Data Breach ("Breach Notice"). Plaintiff's Data Breach is attached as **Exhibit A**.

7. Defendants' Breach Notice obfuscated the nature of the breach and the threat it posted—refusing to tell its victims how many people were impacted, how the breach happened, or why it took the Defendants four months after discovering the Breach to begin notifying victims that hackers had gained access to highly private Sensitive Information.

8. Defendants' failure to timely detect and report the Data Breach made their victims vulnerable to identity theft without any warnings to monitor their financial accounts or credit reports to prevent unauthorized use of their Sensitive Information.

9. Defendants knew or should have known that each victim of the Data Breach deserved prompt and efficient notice of the Data Breach and assistance in mitigating the effects of Sensitive Information misuse.

10. In failing to adequately protect patients' information, adequately notify them about the breach, and obfuscating the nature of the breach, Defendants violated state law and harmed an

unknown number of Corewell's current and former patients.

11. Plaintiff and members of the proposed Class are victims of Defendants' negligence and inadequate cyber security measures. Specifically, Plaintiff and members of the proposed Class trusted Defendants with their Sensitive Information. But Defendants betrayed that trust. Defendants failed to properly use up-to-date security practices to prevent the Data Breach.

12. Plaintiff is a Data Breach victim.

13. Accordingly, Plaintiff, on her own behalf and on behalf of a class of similarly situated individuals, brings this lawsuit seeking injunctive relief, damages, and restitution, together with costs and reasonable attorneys' fees, the calculation of which will be based on information in Defendants' possession.

PARTIES

14. Plaintiff, Joni Lipson, is a natural person and citizen of Michigan, residing in Bloomfield Hills, Michigan, where she intends to remain. Ms. Lipson is a Data Breach victim, receiving Defendants' Breach Notice on November 17, 2023.

15. Defendant, Welltok, is a Colorado limited liability corporation with its principal place of business at 9197 W 6th Ave Ste 600, Denver, CO 80215, US.

16. Defendant, Corewell, is a Michigan corporation with its principal place of business at 26901 Beaumont Boulevard, 6D, Southfield, MI 48033.

JURISDICTION & VENUE

17. This Court has subject matter jurisdiction over this action under 28 U.S.C.§ 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs; there are more than 100 members in the proposed class; At least one Defendant and Plaintiff are citizens of different states.

18. This Court has personal jurisdiction over Defendants because at least one Defendant maintains its principal place of business in this District and does substantial business in this District.

19. Venue is proper in this District under 28 U.S.C. § 1391(b)(2) because a substantial part of the events or omissions giving rise to the claim occurred in this District.

BACKGROUND FACTS

Welltok

20. Welltok is a SaaS company that provides healthcare consumer activation platforms to its clients[1], and advertises itself as an "award winning consumer activation company [that] healthcare organizations and others trust"[2]. Welltok boasts $339 million in annual revenue.[3]

21. Welltok services are specialized for healthcare companies, including Corewell, who oversee highly sensitive data. Welltok thus must oversee, manage, and protect the Sensitive Information of its clients' patients.

22. On information and belief, these third-party patients, whose Sensitive Information was collected by Welltok, do not do any business with Welltok.

23. After collecting patients' Sensitive Information, Welltok maintains the Sensitive Information in its computer systems.

24. As a self-proclaimed leader in its field that regularly handles highly sensitive aspects of its clients' business, Welltok understood the need to protect its client's patients' data

[1] Welltok, Bessemer Venture Partners, https://www.bvp.com/companies/welltok (last visited January 8, 2024).
[2] Welltok. Linkedin, https://www.linkedin.com/company/welltok-inc-/about/ (last visited January 8, 2024).
[3] Welltok, RocketReach, https://rocketreach.co/welltok-a-virgin-pulse-company-profile_b5c0c520f42e085f#:~:text=The%20Welltok%2C%20a%20Virgin%20Pulse,was%20%2483%20million%20in%202023. (last visited January 8, 2024).

and prioritize its data security.

25. Despite recognizing its duty to do so, on information and belief, Welltok has not implemented reasonably cybersecurity safeguards or policies to protect patients' Sensitive Information or trained its IT or data security employees to prevent, detect, and stop breaches of its systems. As a result, Welltok leaves significant vulnerabilities in its systems for cybercriminals to exploit and gain access to patients Sensitive Information.

Corewell

26. Corewell is a healthcare system that "put[s] your health and wellness at our core[.]"[4] Corewell boasts $14 billion in annual revenue. [5]

27. As part of its business, Corewell receives and maintains the Sensitive Information of thousands of current and former patients. In doing so, Corewell implicitly promises to safeguard their Sensitive Information.

28. In collecting and maintaining its current and former patients' Sensitive Information, Corewell agreed it would safeguard the data in accordance with its internal policies, state law, and federal law. After all, Plaintiff and Class Members themselves took reasonable steps to secure their Sensitive Information.

29. Despite recognizing its duty to do so, on information and belief, Corewell has not implemented reasonably cybersecurity safeguards or policies to protect its patients' Sensitive Information or supervised its IT or data security agents and employees, including Welltok, to prevent, detect, and stop breaches of its systems. As a result, Corewell left significant vulnerabilities in its storage of Plaintiff's and the Class's Sensitive Information for cybercriminals

[4] Corehealth, https://corewellhealth.org/about (last visited January 8, 2024).
[5] Corehealth, ZoomInfo, https://www.zoominfo.com/c/corewell-health/566131363 (last visited January 8, 2024).

to exploit and gain access to patients' Sensitive Information.

Defendants Fail to Safeguard Patients' Sensitive Information

30. Plaintiff is a patient of Corewell. As a condition of treatment with Corewell, Plaintiff provided Corewell with her Sensitive Information, including but not limited to her name, date of birth, email address, phone number, diagnosis, health information, and Social Security number. Corewell used that Sensitive Information to facilitate its treatment of Plaintiff and required Plaintiff to provide that Sensitive Information to obtain treatment and care.

31. On information and belief, Corewell provided Welltok with Plaintiff's Sensitive Information as part of the management software services Welltok provided to Corewell. Thus, Welltok was granted access and custody of Plaintiff's Sensitive Information including but not limited to her name, date of birth, email address, phone number, diagnosis, health information, and Social Security number.

32. On information and belief, Defendants collect and maintain patients' Sensitive Information in their computer systems.

33. In collecting and maintaining Sensitive Information, Defendants implicitly agree they will safeguard the data using reasonable means according to state and federal law.

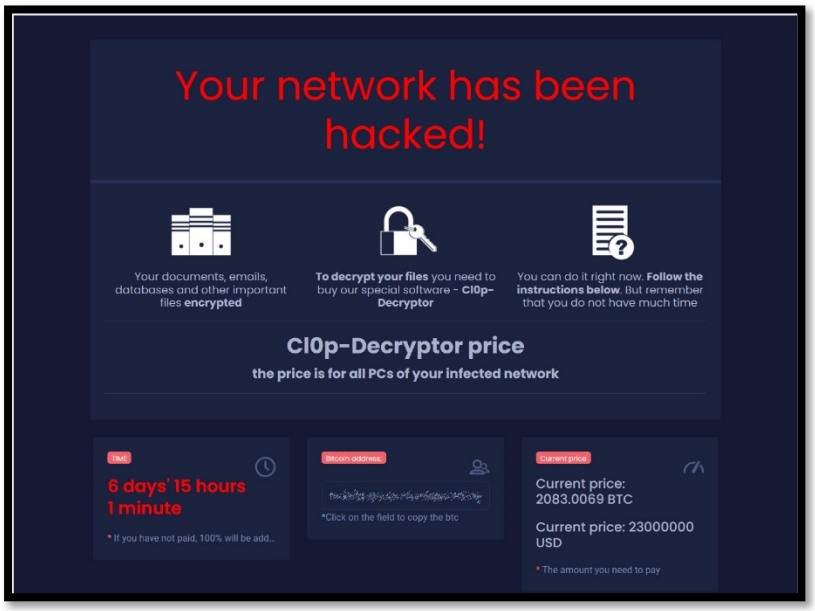
34. According to the Breach Notice, Welltok was informed on July 26, 2023, by its third-party vendor that there was a "software vulnerabilities that [was] made public by the developer of the [third -party software]." Welltok admits that, following an internal investigation, it discovered that "an unknown actor exploited software vulnerabilities […] and exfiltrated certain data [on May 30, 2023.]" Ex. A.

35. In other words, Welltok's investigation revealed that its network had been hacked by cybercriminals and that Defendants' inadequate cyber and data security systems and measures

allowed those responsible for the cyberattack to obtain files containing a treasure trove of thousands of Corewell patients' personal and highly private Sensitive Information. Corewell knew or should have known that granting Welltok access to Plaintiff's Sensitive Information would result in a Data Breach given Welltok's inadequate cybersecurity practices.

36. Upon information and belief, the notorious Clop ransomware gang was responsible for the cyberattack. Ex. A. Clop is one of the most active ransomware actors, having breached over 730 organizations.[6] Defendants, self-touted leaders in their industries, knew or should have known of the tactics that groups like Clop employ.

37. With the Sensitive Information secured and stolen by Clop, the hackers then purportedly issued a ransom demand to Defendants. However, Defendants have provided no public information on the ransom demand or payment. An example of Clop' standard demand ransom for the 'critical vulnerability' found in the third-party software utilized by Defendants is displayed below:



[6] Microsoft Acquired AI-Powered Nuance, Victim of a Cyber Attack, Cybersecurity Express, https://thecyberexpress.com/microsoft-nuance-cyber-attack-clop-ransomware/ (last visited January 8, 2024).

DEAR COMPANIES.

CLOP IS ONE OF TOP ORGANIZATION OFFER PENETRATION TESTING SERVICE AFTER THE FACT.

THIS IS ANNOUNCEMENT TO EDUCATE COMPANIES WHO USE PROGRESS MOVEIT PRODUCT THAT CHANCE IS THAT WE DOWNLOAD ALOT OF YOUR DATA AS PART OF EXCEPTIONAL EXPLOIT. WE ARE THE ONLY ONE WHO PERFORM SUCH ATTACK AND RELAX BECAUSE YOUR DATA IS SAFE.

WE ARE TO PROCEED AS FOLLOW AND YOU SHOULD PAY ATTENTION TO AVOID EXTRAORDINARY MEASURES TO IMPACT YOU COMPANY.

IMPORTANT! WE DO NOT WISH TO SPEAK TO MEDIA OR RESEARCHERS. LEAVE.

STEP 1 - IF YOU HAD MOVEIT SOFTWARE CONTINUE TO STEP 2 ELSE LEAVE.
STEP 2 - EMAIL OUR TEAM UN[redacted] 4 OK[redacted]
STEP 3 - OUR TEAM WILL EMAIL YOU WITH DEDICATED CHAT URL OVER TOR

WE HAVE INFORMATION ON HUNDREDS OF COMPANIES SO OUR DISCUSSION WILL WORK VERY SIMPLE

STEP 1 - IF WE DO NOT HEAR FROM YOU UNTIL JUNE 14 2023 WE WILL POST YOUR NAME ON THIS PAGE
STEP 2 - IF YOU RECEIVE CHAT URL GO THERE AND INTRODUCE YOU
STEP 3 - OUR TEAM WILL PROVIDE 10% PROOF OF DATA WE HAVE AND PRICE TO DELETE
STEP 4 - YOU MAY ASK FOR 2-3 FILES RANDOM AS PROOF WE ARE NOT LYING
STEP 5 - YOU HAVE 3 DAY TO DISCUSS PRICE AND IF NO AGREEMENT YOU CUSTOM PAGE WILL BE CREATED
STEP 6 - AFTER 7 DAYS ALL YOU DATA WILL START TO BE PUBLICATION
STEP 7 - YOU CHAT WILL CLOSE AFTER 10 NOT PRODUCTIVE DAY AND DATA WILL BE PUBLISH

WHAT WARRANTY? OUR TEAM HAS BEEN AROUND FOR MANY YEARS. WE HAVE NOT EVEN ONE TIME NOT DO AS WE PROMISE. WHEN WE SAY DATA IS DELETE IT IS CAUSE WE SHOW VIDEO PROOF. WE HAVE NO USE FOR FEW MEASLE DOLLARS TO DECEIVE YOU.

CALL TODAY BEFORE YOUR COMPANY NAME IS PUBLISH HERE.

FRIENDLY CLOP.

PS. IF YOU ARE A GOVERNMENT, CITY OR POLICE SERVICE DO NOT WORRY, WE ERASED ALL YOUR DATA. YOU DO NOT NEED TO CONTACT US. WE HAVE NO INTEREST TO EXPOSE SUCH INFORMATION.

38. This tactic of exfiltrating the Sensitive Information for a ransom demand before posting Sensitive Information onto a data leak page if the ransom demand is not met is something

Clop, one of the most successful and lucrative ransomware gangs, is well known for.[7] Defendants knew or should have known of the tactics that groups like Clop employ.

39. Despite their duties and alleged commitments to safeguard Sensitive Information, Defendants do not follow industry standard practices in securing patients' Sensitive Information, as evidenced by the Data Breach.

40. In response to the Data Breach, Defendants contend that Welltok will be "reviewing and enhancing our existing policies and procedures related to data privacy[.]" Ex. A. Although Defendants fails to expand on what these alleged "enhancements" are, such enhancements should have been in place before the Data Breach.

41. Through their Breach Notice, Defendants recognized the actual imminent harm and injury that flowed from the Data Breach, so it encouraged breach victims to "remain vigilant against incidents of identity theft and fraud, by regularly reviewing your account statements and monitoring your free credit report [.]"Ex. A.

42. Defendants further recognized their duty to implement reasonable cybersecurity safeguards or policies to protect patients' Sensitive Information, promising that, despite the Data Breach demonstrating otherwise, Welltok, writing "on behalf of Corewell Health East […] remain dedicated to protecting the information in our care." Ex. A.

43. On information and belief, Defendants have offered twelve months of complimentary credit monitoring services to victims during that time, which does not adequately address the lifelong harm that victims will face following the Data Breach. Indeed, the breach involves Sensitive Information that cannot be changed, such as Social Security numbers.

---

[7] Ransomware spotlight: Clop, Trendmicro, https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-clop (last visited January 8, 2024).

44. Even with only twelve months of credit monitoring, the risk of identity theft and unauthorized use of Plaintiff's and Class Members' Sensitive Information is still substantially high. The fraudulent activity resulting from the Data Breach may not come to light for years.

45. Cybercriminals need not harvest a person's Social Security number or financial account information in order to commit identity fraud or misuse Plaintiff's and the Class's Sensitive Information. Cybercriminals can cross-reference the data stolen from the Data Breach and combine with other sources to create "Fullz" packages, which can then be used to commit fraudulent account activity on Plaintiff's and the Class's financial accounts.

46. On information and belief, Defendants failed to adequately train their IT and data security employees on reasonable cybersecurity protocols or implement reasonable security measures, causing it to lose control over their patients' Sensitive Information. Defendants' negligence is evidenced by their failure to prevent the Data Breach and stop cybercriminals from accessing the Sensitive Information.

The Data Breach was a Foreseeable Risk of which Defendants were on Notice.

47. Defendants' data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in the healthcare and healthcare adjacent industry preceding the date of the breach.

48. In light of recent high profile data breaches at other healthcare partner and provider companies, Defendants knew or should have known that their electronic records and patients' Sensitive Information would be targeted by cybercriminals.

49. In 2021, a record 1,862 data breaches occurred, resulting in approximately

293,927,708 sensitive records being exposed, a 68% increase from 2020.[8] The 330 reported breaches reported in 2021 exposed nearly 30 million sensitive records (28,045,658), compared to only 306 breaches that exposed nearly 10 million sensitive records (9,700,238) in 2020.[9]

50. Indeed, cyberattacks against healthcare and healthcare adjacent industries have become increasingly common for over ten years, with the FBI warning as early as 2011 that cybercriminals were "advancing their abilities to attack a system remotely" and "[o]nce a system is compromised, cyber criminals will use their accesses to obtain PII." The FBI further warned that that "the increasing sophistication of cyber criminals will no doubt lead to an escalation in cybercrime." [10]

51. Cyberattacks on medical systems and healthcare partner and provider companies like Defendants' have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets, so they are aware of, and prepared for, a potential attack. As one report explained, "[e]ntities like smaller municipalities and hospitals are attractive. . . because they often have lesser IT defenses and a high incentive to regain access to their data quickly." [11]

52. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in Defendants' industry, including Welltok and Corewell.

---

[8] 2021 Data Breach Annual Report, ITRC, chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.wsav.com/wp-content/uploads/sites/75/2022/01/20220124_ITRC-2021-Data-Breach-Report.pdf (last visited January 8, 2024).

[9] *Id.*

[10] Gordon M. Snow Statement, FBI https://archives.fbi.gov/archives/news/testimony/cyber-security-threats-to-the-financial-sector (last visited January 8, 2024).

[11] Secret Service Warn of Targeted, Law360, https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware (last visited January 8, 2024).

Plaintiff's Experience and Injuries

53. Plaintiff Lipson is a Corewell patient.

54. As a condition of treatment with Corewell, Plaintiff provided it with her Sensitive Information, including but not limited to her name, date of birth, email address, phone number, diagnosis, health information, and Social Security number. Corewell used that Sensitive Information to facilitate its treatment of Plaintiff and required Plaintiff to provide that Sensitive Information to obtain treatment and care.

55. On information and belief, Corewell shared Plaintiff's Sensitive Information with Welltok as part of its provision of management software services to Corewell. Corewell provided Welltok with Plaintiff's Sensitive Information, including but not limited to her name, date of birth, email address, phone number, diagnosis, health information, and Social Security number.

56. Plaintiff provided her Sensitive Information to Defendants and trusted that they would use reasonable measures to protect it according to state and federal law.

57. Defendants deprived Plaintiff of the earliest opportunity to guard herself against the Data Breach's effects by failing to notify her about it for four months.

58. As a result of their inadequate cybersecurity, Defendants exposed Plaintiff's Sensitive Information for theft by cybercriminals and sale on the dark web.

59. As a result of the Data Breach and the recommendation of Defendants' Notice Plaintiff has spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the Notice of Data Breach, and self-monitoring her accounts and credit reports to ensure no fraudulent activity has occurred. This time has been lost forever and cannot be recaptured.

60. Plaintiff has and will spend considerable time and effort monitoring her accounts

to protect herself from identity theft. Plaintiff fears for her personal financial security and uncertainty over what Sensitive Information exposed in the Data Breach. Plaintiff has and is experiencing feelings of anxiety, stress, fear, and frustration because of the Data Breach. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that the law contemplates and addresses.

61. Plaintiff suffered actual injury from the exposure of her Sensitive Information — which violates her rights to privacy.

62. Plaintiff has suffered actual injury in the form of damages to and diminution in the value of her Sensitive Information —a form of intangible property that Plaintiff entrusted to Defendants, which was compromised in and as a result of the Data Breach.

63. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her Sensitive Information being placed in the hands of unauthorized third parties and possibly criminals.

64. Plaintiff has a continuing interest in ensuring that her Sensitive Information, which, upon information and belief, remains backed up in Defendants' possession, is protected, and safeguarded from future breaches.

Plaintiff and the Proposed Class Face Significant Risk of Continued Identity Theft

65. Plaintiff and members of the proposed Class have suffered injury from the misuse of their Sensitive Information that can be directly traced to Defendants.

66. The ramifications of Defendants' failure to keep Plaintiff's and the Class's Sensitive Information secure are severe. Identity theft occurs when someone uses another's personal information such as that person's name, date of birth, Social Security number, or driver's license number, without permission, to commit fraud or other crimes.

67. The types of Sensitive Information compromised and potentially stolen in the Data Breach is highly valuable to identity thieves. The patients' stolen Sensitive Information can be used to gain access to a variety of existing accounts and websites to drain assets, bank accounts or open phony credit cards.

68. Social Security numbers are particularly attractive targets for hackers because they can easily be used to perpetrate identity theft and other highly profitable types of fraud. Moreover, Social Security numbers are difficult to replace, as victims are unable to obtain a new number until the damage is done.

69. Identity thieves can also use the stolen data to harm Plaintiff and Class members through embarrassment, blackmail, or harassment in person or online, or to commit other types of fraud including obtaining ID cards or driver's licenses, fraudulently obtaining tax returns and refunds, and obtaining government benefits. A Presidential Report on identity theft from 2008 states that:

> In addition to the losses that result when identity thieves fraudulently open accounts or misuse existing accounts, . . . individual victims often suffer indirect financial costs, including the costs incurred in both civil litigation initiated by creditors and in overcoming the many obstacles they face in obtaining or retaining credit. Victims of non-financial identity theft, for example, health- related or criminal record fraud, face other types of harm and frustration.
>
> In addition to out-of-pocket expenses that can reach thousands of dollars for the victims of new account identity theft, and the emotional toll identity theft can take, some victims have to spend what can be a considerable amount of time to repair the damage caused by the identity thieves. Victims of new account identity theft, for example, must correct fraudulent information in their credit reports and monitor their reports for future inaccuracies, close existing bank accounts and open new ones, and dispute charges with individual creditors.

70. As a result of Defendants' failure to prevent the Data Breach, Plaintiff and the proposed Class have suffered and will continue to suffer damages, including monetary losses, lost time, anxiety, and emotional distress. They have suffered or are at an increased risk of suffering:

a. The loss of the opportunity to control how their Sensitive Information is used;

b. The diminution in value of the Sensitive Information;

c. The compromise and continuing publication of their Sensitive Information;

d. Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud;

e. Lost opportunity costs and lost wages associated with the time and effort expended addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud;

f. Delay in receipt of tax refund monies;

g. Unauthorized use of stolen Sensitive Information; and

h. The continued risk to their Sensitive Information, which remains in the possession of Defendants and is subject to further breaches so long as Defendants fail to undertake the appropriate measures to protect the Sensitive Information in their possession.

71. Stolen Sensitive Information is one of the most valuable commodities on the criminal information black market. According to Experian, a credit-monitoring service, stolen PII alone can be worth up to $1,000.00 depending on the type of information obtained.

72. The value of Plaintiff's and the proposed Class's Sensitive Information on the black

market is considerable. Stolen Sensitive Information trades on the black market for years, and criminals frequently post stolen Sensitive Information openly and directly on various "dark web" internet websites, making the information publicly available, for a substantial fee of course.

73. It can take victims years to spot identity or Sensitive Information theft, giving criminals plenty of time to use that information for cash.

74. One such example of criminals using Sensitive Information for profit is the development of "Fullz" packages.

75. Cyber-criminals can cross-reference two sources of Sensitive Information to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals. These dossiers are known as "Fullz" packages.

76. The development of "Fullz" packages means that stolen Sensitive Information from the Data Breach can easily be used to link and identify it to Plaintiff and the proposed Class's phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the Sensitive Information stolen by the cyber-criminals in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiff and the Class, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiff and other members of the proposed Class's stolen Sensitive Information is being misused, and that such misuse is fairly traceable to the Data Breach.

77. Defendants disclosed the Sensitive Information of Plaintiff and the proposed Class for criminals to use in the conduct of criminal activity. Specifically, Defendants opened up,

disclosed, and exposed the Sensitive Information of Plaintiff and the Class to people engaged in disruptive and unlawful business practices and tactics, including online account hacking, unauthorized use of financial accounts, and fraudulent attempts to open unauthorized financial accounts (i.e., identity fraud), all using the stolen Sensitive Information.

78. Defendants' use of outdated and insecure computer systems and software that are easy to hack, and their failure to maintain adequate security measures and an up-to-date technology security strategy, as evidenced by their complete failure to prevent malware in their systems, demonstrates a willful and conscious disregard for privacy, and has exposed Sensitive Information of Plaintiff and members of the proposed Class to unscrupulous operators, con-artists, and criminals.

79. Defendants' failure to properly notify Plaintiff and members of the proposed Class of the Data Breach exacerbated Plaintiff's and the Class's injury by depriving them of the earliest ability to take appropriate measures to protect their Sensitive Information and take other necessary steps to mitigate the harm caused by the Data Breach.

Defendants failed to adhere to FTC guidelines.

80. According to the Federal Trade Commission ("FTC"), the need for data security should be factored into all business decision-making. To that end, the FTC has issued numerous guidelines identifying best data security practices that businesses, such as Defendants, should employ to protect against the unlawful exposure of Sensitive Information.

81. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established guidelines for fundamental data security principles and practices for business. The guidelines explain that businesses should:

a. protect the sensitive consumer information that they keep;

b. properly dispose of private information that is no longer needed;

c. encrypt information stored on computer networks;

d. understand their network's vulnerabilities; and

e. implement policies to correct security problems.

82. The guidelines also recommend that businesses watch for large amounts of data being transmitted from the system and have a response plan ready in the event of a breach.

83. The FTC recommends that companies not maintain information longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

84. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect consumer, or in this case, patient data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

85. Defendants' failure to employ reasonable and appropriate measures to protect against unauthorized access to patients' Sensitive Information constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

Defendants Violated HIPAA

86. HIPAA circumscribes security provisions and data privacy responsibilities designed to keep patients' medical information safe. HIPAA compliance provisions, commonly

known as the Administrative Simplification Rules, establish national standards for electronic transactions and code sets to maintain the privacy and security of protected health information.[12]

87. HIPAA provides specific privacy rules that require comprehensive administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of Sensitive Information is properly maintained.[13]

88. The Data Breach itself resulted from a combination of inadequacies showing Defendants' failure to comply with safeguards mandated by HIPAA. Defendants' security failures include, but are not limited to:

a. Failing to ensure the confidentiality and integrity of electronic PHI that it creates, receives, maintains and transmits in violation of 45 C.F.R. § 164.306(a)(1);

b. Failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(2);

c. Failing to protect against any reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3);

d. Failing to ensure compliance with HIPAA security standards by Defendants in violation of 45 C.F.R. § 164.306(a)(4);

---

[12] HIPAA lists 18 types of information that qualify as PHI according to guidance from the Department of Health and Human Services Office for Civil Rights, and includes, *inter alia*: names, addresses, any dates including dates of birth, Social Security numbers, and medical record numbers.

[13] *See* 45 C.F.R. § 164.306 (security standards and general rules); 45 C.F.R. § 164.308 (administrative safeguards); 45 C.F.R. § 164.310 (physical safeguards); 45 C.F.R. § 164.312 (technical safeguards).

e. Failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);

f. Failing to implement policies and procedures to prevent, detect, contain and correct security violations in violation of 45 C.F.R. § 164.308(a)(1);

g. Failing to identify and respond to suspected or known security incidents and failing to mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 C.F.R. § 164.308(a)(6)(ii);

h. Failing to effectively train all staff members on the policies and procedures with respect to PHI as necessary and appropriate for staff members to carry out their functions and to maintain security of PHI in violation of 45 C.F.R. § 164.530(b) and 45 C.F.R. § 164.308(a)(5); and

i. Failing to design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard PHI, in compliance with 45 C.F.R. § 164.530(c).

89. Simply put, the Data Breach resulted from a combination of insufficiencies that demonstrate Defendants failed to comply with safeguards mandated by HIPAA regulations.

Defendants Fail to Comply with Industry Standards

90. As noted above, experts studying cyber security routinely identify entities in possession of Sensitive Information as being particularly vulnerable to cyberattacks because of the value of the Sensitive Information which they collect and maintain.

91. Several best practices have been identified that a minimum should be implemented by companies in possession of Sensitive Information, like Defendants, including but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data and limiting which employees can access sensitive data. Defendants failed to follow these industry best practices, including a failure to implement multi-factor authentication.

92. Other best cybersecurity practices that are standard for companies like Defendants include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points. Defendants failed to follow these cybersecurity best practices, including failure to train staff.

93. Defendants failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

94. These foregoing frameworks are existing and applicable industry standards for a company's obligations to provide adequate data security for its consumers. Upon information and belief, Defendants failed to comply with at least one—or all—of these accepted standards, thereby opening the door to the threat actor and causing the Data Breach.

CLASS ACTION ALLEGATIONS

95. Plaintiff sues on behalf of herself and the proposed nationwide class ("Class"), defined as follows, pursuant to Federal Rule of Civil Procedure 23(b)(2) and (b)(3):

> **All individuals in the United States whose Sensitive Information was accessed without authorization in the Data Breach, including all those who received a notice of the Data Breach.**

96. Excluded from the Class are Defendants, their agents, affiliates, parents, subsidiaries, any entity in which Defendants has a controlling interest, any Defendants officer or director, any successor or assign, and any Judge who adjudicates this case, including their staff and immediate family.

97. Plaintiff reserves the right to amend the class definition.

98. This action satisfies the numerosity, commonality, typicality, and adequacy requirements for suing as representative parties:

99. **Numerosity**. Plaintiff is representative of the proposed Class, consisting of several thousand members, far too many to join in a single action;

100. **Ascertainability**. Class members are readily identifiable from information in Defendants' possession, custody, and control;

101. **Typicality.** Plaintiff's claims are typical of Class member's claims as each arises from the same Data Breach, the same alleged violations by Defendants, and the same unreasonable manner of notifying individuals about the Data Breach.

102. **Adequacy.** Plaintiff will fairly and adequately protect the proposed Class's interests. Their interests do not conflict with Class members' interests, and they have retained counsel experienced in complex class action litigation and data privacy to prosecute this action on the Class's behalf, including as lead counsel.

103. **Commonality.** Plaintiff's and the Class's claims raise predominantly common fact and legal questions that a class wide proceeding can answer for all Class members. Indeed, it will be necessary to answer the following questions:

a. Whether Defendants had a duty to use reasonable care in safeguarding Plaintiff's and the Class's Sensitive Information;

b. Whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

c. Whether Defendants were negligent in maintaining, protecting, and securing Sensitive Information;

d. Whether Defendants breached contract promises to safeguard Plaintiff and the Class's Sensitive Information;

e. Whether Defendants took reasonable measures to determine the extent of the Data Breach after discovering it;

f. Whether Defendants' Breach Notice was reasonable;

g. Whether the Data Breach caused Plaintiff's and the Class' injuries;

h. What the proper damages measure is; and

i. Whether Plaintiff and the Class are entitled to damages, treble damages, or injunctive relief.

104. Further, common questions of law and fact predominate over any individualized questions, and a class action is superior to individual litigation or any other available method to fairly and efficiently adjudicate the controversy. The damages available to individual plaintiffs are insufficient to make individual lawsuits economically feasible.

COUNT I
Negligence
(Against Defendants On Behalf of Plaintiff and the Class)

105. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

106. Plaintiff and members of the Class entrusted their Sensitive Information to Defendants. Defendants owed a duty to Plaintiff and the Class to exercise reasonable care in safeguarding and protecting their Sensitive Information and keeping it from being compromised, lost, stolen, misused, and or/disclosed to unauthorized parties. This duty included, among other things, designing, maintaining, and testing Defendants' security systems to ensure the Sensitive Information of Plaintiff and the Class was adequately secured and protected, including using encryption technologies. Defendants further had a duty to implement processes that would detect a breach of their security system in a timely manner.

107. Defendants were under a basic duty to act with reasonable care when they undertook to collect, create, and store Plaintiff's and the Class's Sensitive Information on their computer system, fully aware–as any reasonable entities of their size would be–of the prevalence of data breaches and the resulting harm such a breach would cause. The recognition of Defendants' duty to act reasonably in this context is consistent with, *inter alia*, the Restatement (Second) of Torts § 302B (1965), which recounts a basic principle: an act or omission may be negligent if the actor realizes or should realize it involves an unreasonable risk of harm to another, even if the harm occurs through the criminal acts of a third party.

108. Defendants knew that the Sensitive Information of Plaintiff and the Class was information that is valuable to identity thieves and other criminals. Defendants also knew of the serious harms that could happen if the Sensitive Information of Plaintiff and the Class was wrongfully disclosed.

109. By being entrusted by Plaintiff and the Class to safeguard their Sensitive Information, Defendants have a special relationship with Plaintiff and the Class. Plaintiff's and the Class's Sensitive Information was provided to Defendants with the understanding that Defendants would take appropriate measures to protect it and would inform Plaintiff and the Class of any security concerns that might call for action by Plaintiff and the Class.

110. Defendants breached their duty to exercise reasonable care in safeguarding and protecting Plaintiff's and the Class members' Sensitive Information by failing to adopt, implement, and maintain adequate security measures to safeguard that information, despite failures and intrusions, and allowing unauthorized access to Plaintiff's and the Class's Sensitive Information.

111. But for Defendants' wrongful and negligent breach of their duties owed to Plaintiff and the Class, their Sensitive Information would not have been compromised, stolen, and viewed by unauthorized persons. Defendants' negligence was a direct and legal cause of the theft of the Sensitive Information of Plaintiff and the Class and all resulting damages.

112. The injury and harm suffered by Plaintiff and the Class members was the reasonably foreseeable result of Defendants' failure to exercise reasonable care in safeguarding and protecting Plaintiff's and the Class members' Sensitive Information.

113. As a result of Defendants' failure, the Sensitive Information of Plaintiff and the Class were compromised, placing them at a greater risk of identity theft and subjecting them to identity theft, and their Sensitive Information was disclosed to third parties without their consent. Plaintiff and Class members also suffered diminution in value of their Sensitive Information in that it is now easily available to hackers on the Dark Web. Plaintiff and the Class have also suffered consequential out of pocket losses for procuring credit freeze or protection services, identity theft monitoring, and other expenses relating to identity theft losses or protective measures.

COUNT II
Negligence *Per Se*
(Against Defendants On Behalf of Plaintiff and the Class)

114. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

115. Pursuant to the FTC Act, 15 U.S.C. § 45, Defendants have a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff's and the Class's Sensitive Information.

116. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendants, of failing to use reasonable measures to protect customer information. The FTC publications and orders promulgated pursuant to the FTC Act also form part of the basis of Defendants' duty to protect Plaintiff and the members of the Class's Sensitive Information.

117. Defendants breached their respective duties to Plaintiff and Class Members under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Sensitive Information.

118. Defendants' duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendants and their patients, which is recognized by laws and regulations including but not limited to HIPAA, as well as common law. Defendants were in a position to ensure that their systems were sufficient to protect against the foreseeable risk of harm to Class Members from a Data Breach.

119. Defendants' duty to use reasonable security measures under HIPAA required Defendants to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(l). Some or all of the

healthcare and/or medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

120. Defendants' duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendants are bound by industry standards to protect confidential Sensitive Information.

121. Defendants violated their duty under Section 5 of the FTC Act by failing to use reasonable measures to protect Plaintiff's and the Class's Sensitive Information and not complying with applicable industry standards as described in detail herein. Defendants' conduct were particularly unreasonable given the nature and amount of Sensitive Information Defendants had collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to individuals in the event of a breach, which ultimately came to pass.

122. The harm that has occurred is the type of harm the FTC Act is intended to guard against. Indeed, the FTC has pursued numerous enforcement actions against businesses that, because of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.

123. Defendants violated their duty under HIPAA by failing to use reasonable measures to protect their PHI and by not complying with applicable regulations detailed supra. Here too, Defendants' conduct was particularly unreasonable given the nature and amount of Sensitive Information that Defendants collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to individuals in the event of a breach, which ultimately came to pass.

124. But for Defendants' wrongful and negligent breach of their duties owed to Plaintiff

and members of the Class, Plaintiff and members of the Class would not have been injured.

125. The injury and harm suffered by Plaintiff and members of the Class were the reasonably foreseeable result of Defendants' breach of their duties. Defendants knew or should have known that Defendants were failing to meet their duties and that their breach would cause Plaintiff and members of the Class to suffer the foreseeable harms associated with the exposure of their Sensitive Information.

126. Had Plaintiff and the Class known that Defendants did not adequately protect their Sensitive Information, Plaintiff and members of the Class would not have entrusted Defendants with their Sensitive Information.

127. Defendants' various violations and their failure to comply with applicable laws and regulations constitute negligence *per se*.

128. As a direct and proximate result of Defendants' negligence *per se*, Plaintiff and the Class have suffered harm, including loss of time and money resolving fraudulent charges; loss of time and money obtaining protections against future identity theft; lost control over the value of Sensitive Information; harm resulting from damaged credit scores and information; and other harm resulting from the unauthorized use or threat of unauthorized use of stolen Sensitive Information, entitling them to damages in an amount to be proven at trial.

129. Additionally, as a direct and proximate result of Defendants' negligence *per se*, Plaintiff and Class members have suffered and will suffer the continued risks of exposure of their Sensitive Information, which remain in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fails to undertake appropriate and adequate measures to protect their Sensitive Information in their continued possession.

COUNT III
Invasion of Privacy
(Against Defendants On Behalf of Plaintiff and the Class)

130. Plaintiff and members of the Class incorporate the above allegations as if fully set forth herein.

131. Plaintiff and the Class had a legitimate expectation of privacy regarding their highly confidential Sensitive Information and were accordingly entitled to the protection of this information against disclosure to unauthorized third parties.

132. Defendants owed a duty to patients, including Plaintiff and the Class, to keep this information confidential.

133. The unauthorized acquisition (i.e., theft) by a third party of Plaintiff and Class members' Sensitive Information is highly offensive to a reasonable person.

134. The intrusion was into a place or thing which was private and entitled to be private. Plaintiff and the Class disclosed their sensitive and confidential information to Defendants, but did so privately, with the intention that their information would be kept confidential and protected from unauthorized disclosure. Plaintiff and the Class were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

135. The Data Breach constitutes an intentional interference with Plaintiff and the Class's interest in solitude or seclusion, either as to their person or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

136. Defendants acted with a knowing state of mind when they permitted the Data Breach because they knew their information security practices were inadequate.

137. Defendants acted with a knowing state of mind when they failed to notify Plaintiff and the Class in a timely fashion about the Data Breach, thereby materially impairing their

mitigation efforts.

138. Acting with knowledge, Defendants had notice and knew that their inadequate cybersecurity practices would cause injury to Plaintiff and the Class.

139. As a proximate result of Defendants' acts and omissions, the Sensitive Information of Plaintiff and the Class were stolen by a third party and is now available for disclosure and redisclosure without authorization, causing Plaintiff and the Class to suffer damages (as detailed *supra*).

140. Unless and until enjoined and restrained by order of this Court, Defendants' wrongful conduct will continue to cause great and irreparable injury to Plaintiff and the Class since their Sensitive Information are still maintained by Defendants with their inadequate cybersecurity system and policies.

141. Plaintiff and the Class have no adequate remedy at law for the injuries relating to Defendants' continued possession of their sensitive and confidential records. A judgment for monetary damages will not end Defendants' inability to safeguard the Sensitive Information of Plaintiff and the Class.

142. In addition to injunctive relief, Plaintiff, on behalf of herself and the other Class members, also seeks compensatory damages for Defendants' invasion of privacy, which includes the value of the privacy interest invaded by Defendants, the costs of future monitoring of their credit history for identity theft and fraud, plus prejudgment interest and costs.

COUNT IV
Breach of Contract
(Against Welltok On Behalf of Plaintiff and the Class)

143. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

144. Defendant Welltok entered into various contracts with healthcare providers,

including Defendant Corewell, to provide software management services to its clients.

145. These contracts are virtually identical to each other and were made expressly for the benefit of Plaintiff and the Class, as it was their confidential medical information that Welltok agreed to collect and protect through its services. Thus, the benefit of collection and protection of the Sensitive Information belonging to Plaintiff and the Class were the direct and primary objective of the contracting parties.

146. Defendant Welltok knew that if it were to breach these contracts with its clients, including Corewell, the clients' patients, including Plaintiff and the Class, would be harmed by, among other things, fraudulent misuse of their Sensitive Information.

147. Defendant Welltok breached its contracts with its clients when it failed to use reasonable data security measures that could have prevented the Data Breach and resulting compromise of Plaintiff's and Class Members' Sensitive Information.

148. As reasonably foreseeable result of the breach, Plaintiff and the Class were harmed by Welltok's failure to use reasonable data security measures to store their Sensitive Information, including but not limited to, the actual harm through the loss of their Sensitive Information to cybercriminals.

149. Accordingly, Plaintiff and the Class are entitled to damages in an amount to be determined at trial, along with their costs and attorney fees incurred in this action.

COUNT V
Breach of Implied Contract
(Against Corewell On Behalf of Plaintiff and the Class)

150. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

151. Plaintiff and the Class delivered their Sensitive Information to Defendant Corewell as part of the process of obtaining treatment and services provided by Corewell.

152. Plaintiff and Class Members entered into implied contracts with Defendant Corewell under which Defendant agreed to safeguard and protect such information and to timely and accurately notify Plaintiff and Class Members if and when their data had been breached and compromised. Each such contractual relationship imposed on Defendant an implied covenant of good faith and fair dealing by which Defendant was required to perform its obligations and manage Plaintiff's and Class Members' data in a manner which comported with the reasonable expectations of privacy and protection attendant to entrusting such data to Defendant.

153. In providing their Sensitive Information, Plaintiff and Class Members entered into an implied contract with Corewell whereby Defendant, in receiving such data, became obligated to reasonably safeguard Plaintiff's and the other Class Members' Sensitive Information.

154. In delivering their Sensitive Information to Corewell, Plaintiff and Class Members intended and understood that Defendant would adequately safeguard that data.

155. Plaintiff and the Class Members would not have entrusted their Sensitive Information to Corewell in the absence of such an implied contract.

156. Corewell accepted possession of Plaintiff's and Class Members' Sensitive Information.

157. Had Corewell disclosed to Plaintiff and Class Members that Defendants did not have adequate computer systems and security practices to secure patients' Sensitive Information, Plaintiff and members of the Class would not have provided their Sensitive Information to Defendant.

158. Corewell recognized that its patients' Sensitive Information is highly sensitive and must be protected, and that this protection was of material importance as part of the bargain to Plaintiff and Class Members.

159. Plaintiff and Class Members fully performed their obligations under the implied contracts with Corewell.

160. Corewell breached the implied contract with Plaintiff and Class Members by failing to take reasonable measures to safeguard its data.

161. Corewell breached the implied contract with Plaintiff and Class Members by failing to promptly notify them of the access to and exfiltration of their Sensitive Information.

162. As a direct and proximate result of the breach of the contractual duties, Plaintiff and Class Members have suffered actual, concrete, and imminent injuries. The injuries suffered by Plaintiff and the Class Members include: (a) the invasion of privacy; (b) the compromise, disclosure, theft, and unauthorized use of Plaintiff's and Class Members' Sensitive Information; (c) economic costs associated with the time spent to detect and prevent identity theft, including loss of productivity; (d) monetary costs associated with the detection and prevention of identity theft; (e) economic costs, including time and money, related to incidents of actual identity theft; (f) the emotional distress, fear, anxiety, nuisance and annoyance of dealing related to the theft and compromise of their Sensitive Information; (g) the diminution in the value of the services bargained for as Plaintiff and Class Members were deprived of the data protection and security that Defendants promised when Plaintiff and the proposed class entrusted Defendants with their Sensitive Information; and (h) the continued and substantial risk to Plaintiff's and Class Members' Sensitive Information, which remains in the Defendants' possession with inadequate measures to protect Plaintiff's and Class Members' Sensitive Information.

COUNT VI
Unjust Enrichment
(Against Defendants On Behalf of Plaintiff and the Class)

163. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

164. This claim is pleaded in the alternative to the breach of implied contracts claim.

165. Plaintiff and members of the Class conferred a benefit upon Defendants in providing Sensitive Information to Defendants.

166. Defendants appreciated or had knowledge of the benefits conferred upon them by Plaintiff and the Class. Defendants also benefited from the receipt of Plaintiff's and the Class's Sensitive Information, as this was used to facilitate the treatment, services, and goods they sold to Plaintiff and the Class.

167. Defendants enriched themselves by saving the costs they reasonably should have expended on data security measures to secure Plaintiff's and Class Members' Sensitive Information.

168. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendants calculated to avoid their data security obligations at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures. Plaintiff and the Class, on the other hand, suffered as a direct and proximate result of Defendants' failure to provide the requisite security.

169. Under the principles of equity and good conscience, Defendants should not be permitted to retain the monetary value of the benefit belonging to Plaintiff and Class Members, because Defendants failed to implement appropriate data management and security measures that are mandated by industry standards.

170. Defendants acquired the monetary benefit and Sensitive Information through inequitable means in that they failed to disclose the inadequate security practices previously alleged.

171. If Plaintiff and Class Members knew that Defendants had not secured Sensitive

Information, they would not have agreed to have their Sensitive Information provided to Defendants.

172. Plaintiff and Class Members have no adequate remedy at law.

173. As a direct and proximate result of Defendants' conduct, Plaintiff and Class Members have suffered and will suffer injury, including, but not limited to: (i) the loss of the opportunity how their Sensitive Information is used; (ii) the compromise, publication, and/or theft of their Sensitive Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their Sensitive Information; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (v) the continued risk to their Sensitive Information, which remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fails to undertake appropriate and adequate measures to protect the Sensitive Information in their continued possession and (vi) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Sensitive Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

174. As a direct and proximate result of Defendants' conduct, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

175. Defendants should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that they unjustly received from them.

PRAYER FOR RELIEF

Plaintiff and members of the Class demand a jury trial on all claims so triable and request that the Court enter an order:

A. Certifying this case as a class action on behalf of Plaintiff and the proposed Class, appointing Plaintiff as class representative, and appointing their counsel to represent the Class;

B. Awarding declaratory and other equitable relief as is necessary to protect the interests of Plaintiff and the Class;

C. Awarding injunctive relief as is necessary to protect the interests of Plaintiff and the Class;

D. Enjoining Defendants from further deceptive practices and making untrue statements about the Data Breach and the stolen Sensitive Information;

E. Awarding Plaintiff and the Class damages that include applicable compensatory, exemplary, punitive damages, and statutory damages, as allowed by law;

F. Awarding restitution and damages to Plaintiff and the Class in an amount to be determined at trial;

G. Awarding attorneys' fees and costs, as allowed by law;

H. Awarding prejudgment and post-judgment interest, as provided by law;

I. Granting Plaintiff and the Class leave to amend this complaint to conform to the evidence produced at trial; and

J. Granting such other or further relief as may be appropriate under the circumstances.

JURY DEMAND

Plaintiff hereby demands that this matter be tried before a jury.

Date: January 8, 2024

Respectfully submitted,

FINK BRESSACK PLLC

/s/ David H. Fink .
David H. Fink (P28235)
Nathan J. Fink (P75185)
38500 Woodward Avenue, Suite 350
Bloomfield Hills, Michigan 48304
(248) 971-2500
dfink@finkbressack.com
nfink@finkbressack.com

By: /s/ Raina Borrelli

TURKE & STRAUSS LLP
Samuel J. Strauss
Raina Borrelli
613 Williamson Street, Suite 201
Madison, Wisconsin 53703
Telephone: (608) 237-1775
Facsimile: (608) 509-4423
sam@turkestrauss.com
raina@turkestrauss.com

Attorneys for Plaintiff and Proposed Class